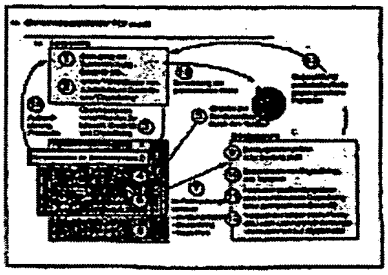
Method for providing franking notes on postal items

Patent number: DE10020402
Publication date: 2001-10-31
Inventor: MEYER BERND (DE); LANG JUERGEN (DE)
Applicant: DEUTSCHE POST AG (DE)
Classification:
- international: G07B17/04; G07B17/02
- european: G07B17/00D2
Application number: DE20001020402 20000427
Priority number(s): DE20001020402 20000427

Also published as:
WO0184505 (A1)
US2004039714 (A1)
CA2427933 (A1)

Abstract of **DE10020402**

The invention relates to a method for providing franking notes on postal items. The invention is characterized in that a credit information number (credit ID - CID) is formed in a loading station, encrypted and then sent to the customer system. The customer system stores the credit information number and the franking note is produced after inputting shipment data. Record of the franking note or notes produced is kept in the customer system.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 20 402 A 1**

(51) Int. Cl.[7]:
G 07 B 17/04
G 07 B 17/02

(21) Aktenzeichen: 100 20 402.3
(22) Anmeldetag: 27. 4. 2000
(43) Offenlegungstag: 31. 10. 2001

DE 100 20 402 A 1

(71) Anmelder:
Deutsche Post AG, 53175 Bonn, DE

(74) Vertreter:
Jostarndt Thul Patentanwälte, 52076 Aachen

(72) Erfinder:
Meyer, Bernd, 53639 Königswinter, DE; Lang, Jürgen, Dr., 51429 Bergisch Gladbach, DE

(56) Entgegenhaltungen:
US 40 97 923
EP 04 00 917 A2
Dr. Stefan Lucks: Vertrauen mit Zertifikat, Funkschau 14/98;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken

(57) Die Erfindung betrifft ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken.
Erfindungsgemäß zeichnet sich das Verfahren dadurch aus, dass in einer Ladestelle eine Kreditierungsinformationsnummer (Credit-ID - CID) gebildet, verschlüsselt und anschließend an das Kundensystem übertragen wird, dass das Kundensystem die Kreditierungsidentifikationsnummer speichert, dass nach Eingabe von Sendungsdaten der Freimachungsvermerk erzeugt wird und dass in dem Kundensystem eine Protokollierung über den angefertigten Freimachungsvermerk und/oder die angefertigten Freimachungsvermerke erfolgt.

DE 100 20 402 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken, wobei ein Kundensystem ein Drucken von Freimachungsvermerken auf Postsendungen steuert.

[0002] Ein gattungsgemässes Verfahren ist aus der internationalen Patentanmeldung WO 98/14907 bekannt.

[0003] Ein weiteres Verfahren ist aus der deutschen Patentschrift DE 31 26 785 C2 bekannt. Bei diesem Verfahren erfolgt eine Erzeugung eines für eine Frankierung von Postsendungen bestimmten Nachladesignals in einem separaten Bereich eines von einem Postbeförderungsunternehmen betriebenen Wertübertragungszentrums.

[0004] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Freimachung von Briefen zu schaffen, das eine hohe Sicherheit des Postversendungsunternehmens mit einer möglichst einfachen Handhabbarkeit durch die Benutzer vereint.

[0005] Erfindungsgemäss wird diese Aufgabe dadurch gelöst, dass in einer Ladestelle eine Kreditierungsinformationsnummer (Credit-ID – CID) gebildet, verschlüsselt und anschliessend an das Kundensystem übertragen wird, dass das Kundensystem die Kreditierungsidentifikationsnummer speichert, dass nach Eingabe von Sendungsdaten Freimachungsvermerke erzeugt werden und dass in dem Kundensystem eine Protokollierung über die angefertigten Freimachungsvermerke versehen mit einer digitalen Signatur erfolgt.

[0006] Die Erfindung sieht insbesondere vor, ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken so durchzuführen, dass der Kunde zuerst die Freimachungsvermerke anfertigt und dass eine Erfassung der angefertigten Freimachungsvermerke, insbesondere ihrer Anzahl, erfolgt.

[0007] Ein wesentlicher Vorteil hierbei ist, dass kein Laden von Freimachungswerten erforderlich ist, sondern dass die tatsächlich hergestellten Freimachungswerte stets im Nachhinein gemeldet und berechnet werden. Durch den vereinfachten Prozess eignet sich eine bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens (PCF credit) insbesondere für Unternehmen mit mittlerem und größerem Sendungsaufkommen und entsprechender Kreditwürdigkeit.

[0008] Zur Erhöhung der Datensicherheit ist es zweckmäßig, dass die Protokollierung des Freimachungsvermerks mit einer digitalen Signatur gekennzeichnet wird.

[0009] Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Zeichnungen.

[0010] Von den Zeichnungen zeigt:

[0011] **Fig.** 1 eine Prinzipdarstellung von in einer ersten Ausführungsform des Verfahrens eingesetzten Sicherheitsmechanismen und

[0012] **Fig.** 2 eine Prinzipdarstellung von in einer weiteren Ausführungsform des Verfahrens eingesetzten Sicherheitsmechanismen.

[0013] Das Verfahren beinhaltet mehrere Schritte, die mit unterschiedlichen Häufigkeiten durchgeführt werden. Einzelne Prozesse wie das Erzeugen eines Freimachungsvermerkes erfolgen häufiger als andere Prozesse, beispielsweise eine Authentisierung des Kundensystems gegenüber einer zentralen Ladestelle. Vorzugsweise erfolgt nach jeder Authentisierung der nachfolgend anhand der Bezugszeichen **1**, **2**, **3** und **4** dargestellte Ladevorgang.

[0014] Die Herstellung der Freimachungsvermerke erfolgt vorzugsweise getrennt von diesem Ladevorgang.

1. In der Ladestelle wird eine Zufallszahl X und eine sogenannte Credit-ID CID gebildet, die Informationen zum Kunden, zur Höhe seiner Kreditwürdigkeit und zum Gültigkeitszeitraum der CID (d. h. zur Häufigkeit des Durchlaufens des Kreisprozesses) enthält.
2. In der Ladestelle werden Zufallszahl X und Credit-ID CID zu einem sogenannten "CryptoString" derart verschlüsselt (z. B. symmetrisch), dass nur das Briefzentrum in der Lage ist, aus diesem CryptoString wieder die Zufallszahl und die CID zu entschlüsseln.
3. Zufallszahl X, Credit-ID CID und der CryptoString werden derart (z. B. asymmetrisch) verschlüsselt, dass nur das Kryptomodul im Kundensystem in der Lage ist, diese Informationen wieder zu entschlüsseln.
4. Im Kryptomodul im Kundensystem werden die Zufallszahl X, die Credit-ID CID und der CryptoString zwischengespeichert. Anschließend kann die Kommunikation mit der Ladestelle beendet werden.
5. Der Kunde gibt im Rahmen der Herstellung von Freimachungsvermerken sendungsspezifische Informationen (z. B. Teile der Anschrift, Postleitzahl, Porto, Sendungsart etc.) in das Kryptomodul ein.
6. Das Kryptomodul erzeugt einen Hash-Wert unter anderem aus den sendungsspezifischen Daten, der Zufallszahl, der Credit-ID CID (und gegebenenfalls weiteren Informationen)
7. Das Kundensystem erzeugt einen Freimachungsvermerk, der unter anderem folgende Informationen enthält: die Sendungsdaten im Klartext, den zwischengespeicherten CryptoString und den erzeugten Hash-Wert.
8. Das Kryptomodul signiert die sicherheitsrelevanten Informationen aus dem Freimachungsvermerk digital mit dem eigenen privaten Schlüssel und legt sie in einer Protokolldatei im Kundensystem ab.
9. Im Briefzentrum erfolgt zunächst eine Prüfung auf Plausibilität; hierzu werden die sendungsspezifischen Daten des Freimachungsvermerks mit den Eigenschaften der Sendung verglichen.
10. In einem weiteren Prüfschritt wird der CryptoString, der so verschlüsselt war, dass nur das Briefzentrum diesen entschlüsseln konnte, zu Zufallszahl X und Credit-ID CID entschlüsselt.
11. Ebenso wie das Kundensystem bildet nun das Briefzentrum einen Hash-Wert, unter anderem aus den sendungsspezifischen Daten, der aus dem CryptoString entschlüsselten Zufallszahl und Credit-ID CID (und gegebenenfalls weiteren Informationen).
12. Durch einen Vergleich des soeben selbst erzeugten Hash-Wertes mit dem im Freimachungsvermerk empfangenen Hash-Wert wird festgestellt, ob das zur Herstellung des Freimachungsvermerk tatsächlich das (vertrauenswürdige) Kryptomodul im Kundensystem verwendet wurde, womit die Gültigkeit des Freimachungsvermerks belegt wird.
13. In einer Gegenprüfung können die produzierten (im Briefzentrum verarbeiteten) Werte an die Ladestelle gemeldet werden.
14. Die Abrechnung der hergestellten Freimachungsvermerke erfolgt im Rahmen der regelmäßigen Kontaktierung der Ladestelle durch das Kundensystem. Hierbei wird das Kryptomodul im Kundensystem authentisiert. In diesem Zusammenhang werden die unter Punkt **8** erstellten, digital signierten Protokolldaten an die Ladestelle übergeben.
15. Die übergebenen Protokolldaten werden herangezogen, um die hergestellten Freimachungsvermerke dem Kunden in Rechnung zu stellen. Nach der Übertra-

gung der Protokolldaten in Punkt **14** kann wieder mit Punkt **1**, das heißt, mit der Vorbereitung einer neuen Zufallszahl X und einer neuen Credit-ID CID, fortgefahren werden.

[0015] Nachfolgend wird anhand von **Fig. 2** eine Variante des erfindungsgemäßen Verfahrens dargestellt, die sich durch eine vereinfachte Durchführung auszeichnet. Die Vereinfachung bringt Vorteile bezüglich der möglichen Geschwindigkeit bei der Herstellung von Freimachungsvermerken beim Kunden mit sich. Um das potentiell niedrigere Sicherheitsniveau, das mit dieser Art der Freimachung erzielt werden kann, auszugleichen, ist zum Einen eine spezielle Einlieferungsform (z. B. Verzicht auf anonyme Briefkasteneinlieferung) erforderlich, bei der die eingelieferte Menge festgestellt werden kann. Zusammen mit einer besonderen Kreditwürdigkeit des Kunden eignet sich dieses Verfahren insbesondere für große und sehr große Sendungsmengen.

[0016] Bei dem in **Fig. 2** dargestellten Prozess handelt es sich vorzugsweise um einen Kreisprozess, der regelmäßig. z. B. täglich, durchlaufen wird. Der eigentliche Beginn des Kreispozesses ist der in der Abbildung mit Nr. 12 gekennzeichnete Schritt der Authentisierung des Kundensystems gegenüber einer zentralen "Ladestelle". Aus Gründen der einfacheren Darstellbarkeit beginnt in dieser Darstellung der Kreisprozess jedoch erst nach erfolgter Authentisierung mit dem ersten Prozesschritt:

1. In der Ladestelle wird eine sogenannte Credit-ID CID gebildet, die Informationen zum Kunden, zur Höhe seiner Kreditwürdigkeit und zum Gültigkeitszeitraum der CID (d. h. zur Häufigkeit des Durchlaufens des Kreisprozesses) enthält.
2. In der Ladestelle wird die Credit-ID CID zum sogenannten "CryptoCredit" derart verschlüsselt (z. B. symmetrisch), dass nur das Briefzentrum in der Lage ist, aus diesem CryptoCredit wieder die CID zu entschlüsseln.
3. Credit-ID CID und CryptoCredit werden derart (z. B. asymmetrisch) verschlüsselt, dass nur das Kryptomodul im Kundensystem in der Lage ist, diese Informationen wieder zu entschlüsseln.
4. Im Kryptomodul im Kundensystem werden Credit-ID CID und CryptoCredit zwischengespeichert. Anschließend kann die Kommunikation mit der Ladestelle beendet werden.
5. Der Kunde gibt im Rahmen der Herstellung eines Freimachungsvermerks sendungsspezifische Informationen (z. B. Teile der Anschrift, Postleitzahl, Porto, Sendungsart etc.) in das Kryptomodul ein.
6. Das Kryptomodul erzeugt eine digitale Signatur für die sicherheitsrelevanten Informationen, die auch in den Freimachungsvermerk (vgl. Punkt 7) einfließen.
7. Das Kundensystem erzeugt einen Freimachungsvermerk, der unter anderem folgende Informationen enthält: die Sendungsdaten im Klartext und den zwischengespeicherten CryptoCredit.
8. Das Kryptomodul legt die mit dem eigenen privaten Schlüssel digital signierten sicherheitsrelevanten Informationen aus dem Freimachungsvermerk in einer Protokolldatei im Kundensystem ab.
9. Im Briefzentrum erfolgt bei der Einlieferung eine Ermittlung der Sendungsmenge. Aus den eingelieferten Sendungen können Stichproben zur Gültigkeitsprüfung genommen werden.
10. Im Rahmen einer vereinfachten Gültigkeitsprüfung wird der CryptoCredit, der so verschlüsselt war, dass nur das Briefzentrum diesen entschlüsseln konnte, zur Credit-ID CID entschlüsselt. Hierdurch kann eine Gültigkeit der Credit-ID und eine Zuordnung zum registrierten Kunden geprüft werden.
11. Zur Gegenprüfung wird die Zahl der eingelieferten Sendungen an die Ladestelle gemeldet.
12. Die Abrechnung des hergestellten Freimachungsvermerks erfolgt im Rahmen der regelmäßigen Kontaktierung der Ladestelle durch das Kundensystem. Hierbei wird das Kryptomodul im Kundensystem authentisiert. In diesem Zusammenhang werden die unter Punkt **8** erstellten, digital signierten Protokolldaten an die Ladestelle übergeben.
13. Die übergebenen Protokolldaten werden herangezogen, um dem hergestellten Freimachungsvermerk dem Kunden in Rechnung zu stellen. Nach der Übertragung der Protokolldaten in Punkt **12** kann wieder mit Punkt **1**, d. h. der Vorbereitung einer neuen Zufallszahl X und einer neuen Credit-ID CID, fortgefahren werden.

[0017] Die erfindungsgemäßen Verfahren ermöglichen eine Frankierung von Postsendungen bei größtmöglicher Benutzerfreundlichkeit für die Anwender und mit einer hohen Entgeltsicherheit für das Postbeförderungsunternehmen.

Patentansprüche

1. Verfahren zum Versehen von Postsendungen mit einem Freimachungsvermerk, wobei ein Kundensystem ein Drucken eines Freimachungsvermerks auf Postsendungen steuert, **dadurch gekennzeichnet**, dass in einer Ladestelle eine Kreditierungsinformationsnummer (Credit-ID - CID) gebildet, verschlüsselt und anschliessend an das Kundensystem übertragen wird, dass das Kundensystem die Kreditierungsidentifikationsnummer speichert, dass nach Eingabe von Sendungsdaten der Freimachungsvermerk erzeugt wird und dass in dem Kundensystem eine Protokollierung über den angefertigten Freimachungsvermerk und/oder die angefertigten Freimachungsvermerke erfolgt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Protokollierung des Freimachungsvermerks mit einer digitalen Signatur gekennzeichnet wird.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 20 402 A1
Int. Cl.[7]: G 07 B 17/04
Offenlegungstag: 31. Oktober 2001

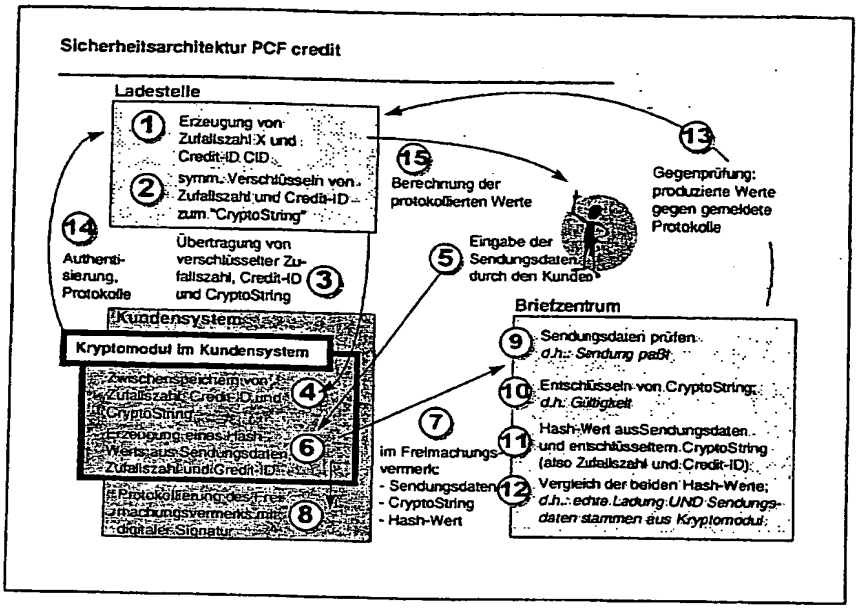


Fig. 1

Nummer: DE 100 20 402 A1
Int. Cl.[7]: G 07 B 17/04
Offenlegungstag: 31. Oktober 2001

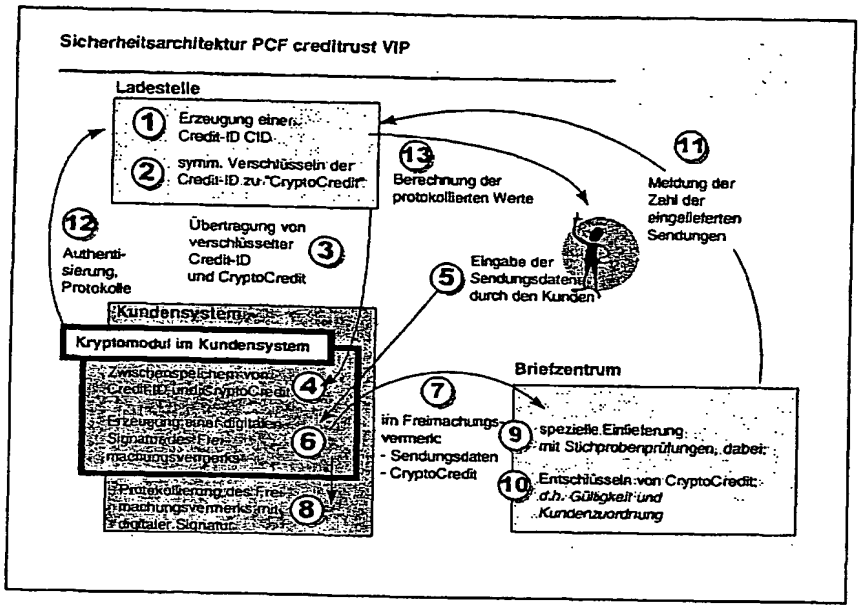


Fig. 2